



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,547	06/06/2000	TARO TERA0	106408	8229
25944	7590	03/31/2005	EXAMINER	
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 03/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/588,547

Applicant(s)

TERAO, TARO

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 February 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) 21-38 is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 June 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☒ Interview Summary (PTO-413)
Paper No(s)/Mail Date. 20050324.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-38 have been examined. The amendment received on 1/26/05 has been entered. Claims 1, 5, 7, 20, 21, 24, 25, 26, 28, 31 and 33 were amended.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/24/05 has been entered.

Response to Arguments

3. The following is a response to the arguments presented by the applicant on pages 13-21 in the amendment filed on January 26, 2005 (hereinafter Remarks). Those arguments not addressed below can be found in the advisory action dated February 7, 2005.

4. In reply to applicant's argument that the prior art of record does not teach or suggest the limitations defined by the instant independent claims (Remarks, pgs. 13-20), examiner respectfully disagrees; after further consideration of the Zhang prior art, a

Art Unit: 2132

new ground(s) of rejection is issued, which covers all new limitations of claims 1-20, as outlined below.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 2, 5-10 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang U.S. Patent No. 6,154,541 (hereinafter Zhang).

7. As per claim 1, Zhang covers a method for generating a one-way-function value by applying a one-way-function to a plurality of seed values to create a hash value. These seed values and the resulting hash value cover the values u , M , and $X(M)$ as defined by applicant's claim 1. (col. 22:37-46) Although Zhang does not explicitly define combining a unique value d and a unique value s to create the unique value u , Zhang does teach strategies of combining a plurality of parameters to generate new parameters using the following methods as disclosed in col. 21:65-22:36 to ensure a more secure key generation methodology:

- a. Segmented sequences
- b. Reassembling of fragmented/fractured numbers

- c. Multi-seeding
- d. Reseeding
- e. Any combinations of the above 4

Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to create a unique value u from the values s and d since it hinders disclosure of the generated keys by attempts to surreptitiously analyze the key generator as taught by Zhang, *ibid*. Further, Zhang discloses the seed values and resulting hash value defined in relation to vector spaces, which covers values of $u = (u_1 \dots u_m)$ and $X(M)$ as a concatenation of m hashes on M and u . (col. 13:12-14:60, especially 14:45-50; 9:62-10:13; 10:20-23; standard hash functions such as MD3-5 and N-Hash take as input a plurality of values and output a concatenation of a plurality of values) Moreover, seed values are for a user (13:10; users can provide passwords as a seed); all values are held by a right issuer, wherein the right issuer issues a capability X to the user, the capability X representing a right of the user in association with the message M (12:65-13:46; the crypt unit holds the seed values and resulting key values); the unique value u is provided to a user creating the one-way function value $X(M)$ as a way to establish a right for a user wherein the user verified from a public key y and a capability X by a right verifier. (5:55-6:40; 13:9-18; 30:53-34:17, especially 30:55-32:5) The aforementioned cover the limitations of claim 1.

8. As per claim 2, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. In addition, Zhang discloses means wherein the value generation unique value

Art Unit: 2132

u is calculated by applying a one-way function G to the function generation unique value s and the unique value d. (Col. 22:31-36)

9. As per claims 5 and 6, the rejections of claim 2 under 35 U.S.C. 103(a) are incorporated herein. In addition, Zhang teaches that the steps defined above can be implemented in a smart card. (Col. 6:27; 13:3) The aforementioned cover claims 5 and 6.

10. As per claims 7-9, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. In addition, Zhang covers a proving device for performing processing based on a private key dependent on a message M (col. 6:19-40, especially line 25) and the device covers means for performing processing based on the private key X(M). (fig. 2, 'Crypt Unit B', and related text) The aforementioned cover the limitations of claims 7-9.

11. As per claim 10, the rejection of claim 7 under 35 U.S.C. 103(a) is incorporated herein. Zhang does not expressly disclose that the proving device is configured as a module inside a CPU of the device. Examiner takes Official Notice that proving devices, especially those using private keys in a cryptosystem, are conventionally configured as a module inside a CPU of a device. It would be obvious to one of ordinary skill in the art at the time the invention was made to configure the proving device as a module inside a CPU of the device since processors are the standard means of implementing a

cryptographic proving device as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 10.

12. As per claim 19, the rejection of claim 7 under 35 U.S.C. 103(a) is incorporated herein. In addition, Zhang teaches that parameters defined by the method can be specified as variables controlling both the system and the keys generated. (Zhang, col. 16:44-45)

13. As per claim 20, it is an apparatus claim corresponding to claim 19 and it does not teach or define above the information claimed in claim 19. Therefore, claim 20 is rejected under Zhang for the same reasons set forth in the rejections of claim 19.

14. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang, and further in view of Stallings Cryptography and Network Security Chapter 11, "Authentication Applications" (hereinafter Stallings).

15. As per claim 18, the rejection of claim 7 under 35 U.S.C. 103(a) is incorporated herein. Zhang is silent on the message M including use conditions of the message by the method. Stallings teaches use conditions of a message in the analogous art of digital certificates. In particular, X.509 certificates define use conditions in the extensions to the standard parameters on the information established in the certificate. Stallings, pg. 348, bullet 'Key usage'. As such, use conditions specifying the policies

Art Unit: 2132

under which the values can be used or processed would be obvious to one of ordinary skill in the art at the time the invention was made since it enables a flexible means by which to distribute a plurality of types of messages and ensure that values distributed are properly processed or used. Stallings, *ibid.* The aforementioned cover the limitations of claim 18.

16. Claims 3, 4, and 11-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang in view of Schneier Applied Cryptography Chapters 1, 11, 12, 19, 20 and 21 (hereinafter Schneier).

17. As per claim 3, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. In addition, Zhang discloses scrambling s and d to create value u (col. 22, lines 31-36), but does not expressly disclose an encryption function with a symmetric key as the scrambling operation. However as taught by Schneier, scrambling techniques, such as diffusion and confusion, are commonly executed by symmetric encryption algorithms. (pg. 237, 'Confusion and Diffusion'; pgs. 270-278, section 12.2 'Description of DES', especially 'Expansion Permutation' and 'S-Box Substitution') It would be obvious to one of ordinary skill in the art at the time the invention was made to apply an encryption function with a symmetric key as the scrambling operation since it utilizes a simple but efficient encryption scheme to scramble s and d to create u to establish a secure encryption function. Schneier, *ibid.* The aforementioned cover the limitations of claim 3.

18. As per claim 4, Zhang covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a) is incorporated herein. Zhang does not expressly disclose calculating $X(M)$ by applying both the one-way function H and an encryption function D of a symmetric key to the values u and M . However, as known in the art, encryption steps using symmetric keys are efficient means to hide sensitive values (see Schneier, pg. 4, 'Symmetric Algorithms'). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to also apply an encryption function D of a symmetric key to the values u and M since it ensures a greater degree of security on the processed values. Schneier, *ibid*. The aforementioned cover the limitations of claim 4.

19. As per claims 11-17, the rejections of claim 7 under 35 U.S.C. 103(a) is incorporated herein. In addition, the processing steps by the proving device as listed in dependent claims 11-17 are generic implementations of well-established cryptosystems as taught by Schneier. In summary, claims 11 and 12 are processing means to implement any type of verification scheme using a challenge variable such as a DSA signature algorithm (Schneier, pgs. 486-487, 'Description of DSA', where $H(m)$ is the challenge variable); claims 13-14 are processing means to implement authentication schemes having commitment values such as the Schnorr authentication (Schneier, pg. 511, 'Authentication Protocol', where x is the commitment); claims 15 and 17, read on encryption schemes using multiplication, power operations, and modular arithmetic,

Art Unit: 2132

including DSA signature and Schnorr authentication schemes as listed earlier; and finally, claim 16 reads on operations using elliptic curve cryptosystems (Schneier, pg. 480, section 19.8). It would be obvious to one of ordinary skill in the art at the time the invention was made to perform the processing based on standard cryptosystems since it ensures that the proving device is derived from proven cryptosystems. Schneier, *ibid*. The aforementioned cover the limitations of claims 11-17.

Allowable Subject Matter

20. Claims 21-38 are allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

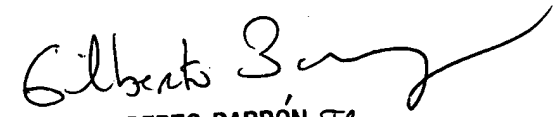
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
March 25, 2005



GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100